(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－83847

(43)公開日　平成６年(1994)３月25日

(51)Int.Cl.[5]		識別記号	庁内整理番号	FI	技術表示箇所
Ｇ０６Ｆ	15/21	３６０	7052－5L		
	12/00	５３７　Ｄ	8526－5B		
	12/14	３１０　Ｋ	9293－5B		

審査請求　未請求　請求項の数12(全　８　頁)

(21)出願番号　特願平4－236867

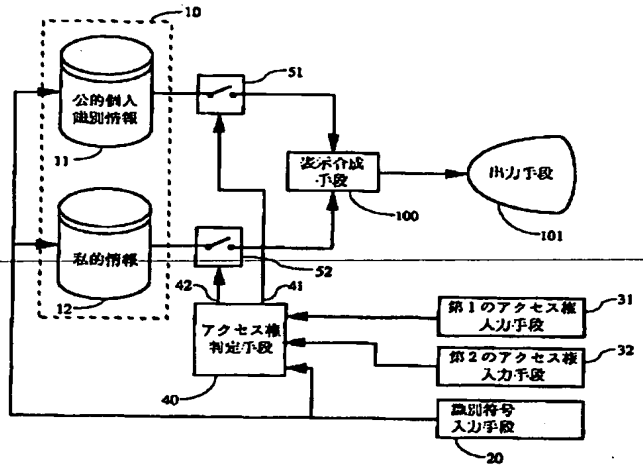
(22)出願日　平成４年(1992)９月４日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　相坂　一夫
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　橘詰　明英
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　個人情報保護方法およびその装置

(57)【要約】
【構成】データ記憶手段１０の内容を、患者氏名等の公的個人識別情報１１と診療データ等の私的情報１２に分け、各々へのアクセスに対して独立な制限手段５１，５２を設ける。両制限手段の制御は、患者のアクセス同意を示す第１のアクセス権入力手段３１による入力，医師のアクセス権限を示す第２のアクセス権入力手段３２による入力，患者ＩＤを示す識別符号入力手段による入力の組合せに応じてアクセス権判定手段４０が行なう。
【効果】診療データが氏名入りで漏洩することを防止できる。

図２



1

【特許請求の範囲】

【請求項１】不特定多数の個人情報を集めて記憶する個人情報記憶手段と、上記個人情報記憶手段に記憶された特定の個人又は集団の個人情報にアクセスするために上記個人又は集団の個人識別符号を入力するための識別符号入力手段と、上記個人情報にアクセスすることが正当であることを主張するアクセス権を入力するアクセス権入力手段と、上記各入力手段から入力された上記アクセス権と上記個人識別符号を照合し、上記アクセスが正当か否かを判定するアクセス権判定手段と、上記アクセス権判定手段の判定結果に基づき上記個人情報記憶手段へのアクセス又は上記個人情報記憶手段からの出力を制限するアクセス制限手段とを備える個人情報保護方法において、上記個人情報記憶手段は各個人を社会的に識別する公的個人識別情報と各個人に固有の私的情報とを含み、上記アクセス制限手段は上記公的個人識別情報と上記私的情報について各々独立にアクセス制限を行なう公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とからなり、上記アクセス権判定手段は、上記各入力手段から入力されたアクセス権と個人識別符号を照合した結果、上記公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与えることを特徴とする個人情報保護方法。

【請求項２】請求項１において、上記私的情報は個人の医療データである個人情報保護方法。

【請求項３】請求項２において、上記アクセス権入力手段は、患者が携帯し上記個人識別符号を保持する患者識別媒体から上記個人識別符号を入力する第１のアクセス権入力手段および医師が携帯し上記アクセス権を保持する医師識別媒体から上記アクセス権を入力する第２のアクセス権入力手段からなり、上記アクセス権判定手段は、上記第１のアクセス権入力手段から入力された第１の個人識別符号と、上記識別符号入力手段から入力された第２の個人識別符号と、上記第２のアクセス権入力手段から入力されたアクセス権とからなる組合せに従って上記公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与える個人情報保護方法。

【請求項４】請求項３において、上記アクセス権判定手段は、上記第１の個人識別符号と第２の個人識別符号とが双方入力され、かつ両者が異なる場合は公的個人識別情報と私的情報との双方へのアクセスを制限すること、上記第１の個人識別符号と第２の個人識別符号とが双方入力され、両者が一致する場合は上記アクセス権の入力状況に従って、アクセス権が入力されない場合は、私的情報へのアクセスを制限し、アクセス権が入力された場合は、公的個人識別情報と私的情報双方に対しアクセスを制限しないこと、および上記第１の個人識別符号が入力されない場合は上記アクセス権の入力状況に従って、アクセス権が上記患者の主治医のアクセスであることを主張する場合には、公的個人識別情報と私的情報双方に対しアクセスを制限せず、アクセス権が主治医以外の者のアクセスであることを主張する場合には、公的個人識別情報へのアクセスを制限することにより、上記公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与える個人情報保護方法。

2

【請求項５】請求項３または４において、上記患者識別媒体は、医療機関が受診者に発行する診察券を兼ねる個人情報保護方法。

【請求項６】請求項３または４において、上記患者識別媒体は、患者個人が携帯し上記患者の長期間にわたる診療情報を記録する媒体である個人情報保護方法。

【請求項７】請求項３または４において、上記医師識別媒体は、上記医師の身分証明書を兼ねる個人情報保護方法。

【請求項８】請求項２，３，４，５，６または７に記載の個人情報保護方法を用いる電子カルテシステム。

【請求項９】請求項１に記載の個人情報保護方法を実行する個人情報保護装置。

【請求項１０】請求項９において、各個人を社会的に識別する公的個人識別情報と各個人に固有の私的情報とを含む個人情報記憶装置と、この記憶装置に記憶された特定の個人又は集団の個人情報にアクセスするために上記個人又は集団の個人識別符号を入力するための識別符号入力装置と、上記個人情報にアクセスすることが正当であることを主張するアクセス権を入力するアクセス権入力装置と、上記公的個人識別情報へのアクセスを制限する公的個人識別情報アクセス制限装置と、上記私的情報へのアクセスを制限する私的情報アクセス制限装置と、上記各入力装置から入力されたアクセス権と個人識別符号を照合した結果、上記公的個人識別情報アクセス制限装置と私的情報アクセス制限装置とに独立のアクセス権判定結果を与えるアクセス権判定装置とを備えた個人情報保護装置。

【請求項１１】請求項３に記載の個人情報保護方法を実行する個人情報保護装置。

【請求項１２】請求項１１において、患者が携帯し上記個人識別符号を保持する患者識別媒体から上記個人識別符号を入力する第１のアクセス権入力装置と、医師が携帯し上記アクセス権を保持する医師識別媒体から上記アクセス権を入力する第２のアクセス権入力装置と、上記第１のアクセス権入力装置から入力された第１の個人識別符号と、上記識別符号入力装置から入力された第２の個人識別符号と、上記第２のアクセス権入力装置から入力されたアクセス権とからなる組合せに従って上記公的個人識別情報アクセス権制限装置と私的情報アクセス権制限装置とに独立のアクセス権判定結果を与えるアクセス権判定装置とを備えた個人情報保護装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はデータベースシステムに利用される個人情報保護方法およびその装置に係り、特に、病院向け診療情報データベースなどの高度の情報保護を必要とする個人情報保護方法及びその装置に関する。

【０００２】

【従来の技術】カルテ等の医療データを電子化して記憶・管理することにより、診療業務の効率化を図るシステムが現在開発されつつある。ここで扱われる医療データは個人のプライバシーに関する情報であり、医師法を初めとして多くの関連法規で守秘義務が定められている。このため、個人医療データのアクセスに制限を加えることでプライバシーの保護を図る個人情報保護方法がシステムに採用される。情報保護方法の具体的な例として、次の二つの公知例をあげることができる。

【０００３】第１は医療データ向けの例であり、第６回医療情報学連合大会において、東京大学の渡邊らにより講演された「東大病院における患者データの機密保護」（講演番号３－Ａ－１３）である。同方法の概要は（１）システム利用者にはシステム管理者がＩＤカードを発行し、カードは使用者の職種（医師，看護婦，技師，事務職）により区分され、（２）システム利用時には、管理者はＩＤカードをチェックし、利用者の職種および所属診療科に従って許された患者の情報のみをアクセスできる点にある。

【０００４】第２の例として、医療データに関するものではないが、現在広く実用化されている銀行預金残高の照会システムをあげることができる。同システムでは残高照会の際に預金者本人であることを示す暗証番号を入力することで、情報が第３者に漏洩することを防いでいる。

【０００５】この二つの公知例は、いずれも図３に示す形式で個人情報保護を行なっている。すなわち、利用者は個人識別符号およびアクセス権情報を二つの入力手段２０，３０から入力し、記憶手段１０中の個人情報にアクセスする。アクセスの正当性はアクセス権判定手段４０で判定され、判定結果４０１がアクセス制限手段５００を制御することで情報が出力手段１０１に送られるのを防いでいる。なお、第１の公知例の場合の様に、２０と３０は物理的に同一の入力装置であっても良い。

【０００６】

【発明が解決しようとする課題】しかし第１の公知例では、アクセスに患者の同意を必要としないため、自己の情報が漏洩することを患者自身が防止する手段がない点に問題がある。一方、第２の公知例では、情報が漏洩する危険は小さいが、医療データのアクセスに常に患者の同意を要し、医師が患者の症例を研究・検討する際に大きな妨げになる。一般に医学研究では、患者のプライバシーを侵さない範囲において症例を研究することは医療

の進歩に必須の手段として認められている。すなわち、第２の公知例による個人情報保護方法は、医療の進歩を著しく阻害するという問題を持つ。

【０００７】本発明の目的は、患者のプライバシー保護と医学研究との双方に有効な個人情報保護方法およびその装置を提供することにある。

【０００８】

【課題を解決するための手段】上記課題は、個人情報記憶手段の記憶内容を、各個人を社会的に識別する公的個人識別情報と各個人に固有の私的情報とに区分し、これらに、（１）同記憶手段に記憶された特定の個人又は集団の個人情報にアクセスするために上記個人又は集団の個人識別符号を入力するための識別符号入力手段、（２）上記個人情報にアクセスすることが正当であることを主張するアクセス権を入力するアクセス権入力手段、（３）上記公的個人識別情報へのアクセスを制限する公的個人識別情報アクセス制限手段、（４）上記私的情報へのアクセスを制限する私的情報アクセス制限手段、（５）上記各入力手段から入力されたアクセス権と個人識別符号を照合した結果、上記公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与えるアクセス権判定手段の各手段を適用することにより解決する。

【０００９】また、上記アクセス権入力手段は、患者が携帯し上記個人識別符号を保持する患者識別媒体から上記個人識別符号を入力する第１のアクセス権入力手段と、医師が携帯し上記アクセス権を保持する医師識別媒体から上記アクセス権を入力する第２のアクセス権入力手段の２者からなっていても良い。この場合、上記アクセス権判定手段は、上記第１のアクセス権入力手段から入力された第１の個人識別符号と、上記識別符号入力手段から入力された第２の個人識別符号と、上記第２のアクセス権入力手段から入力されたアクセス権とからなる組合せに従って上記公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与える。

【００１０】なお、以上の説明で公的個人識別情報とは、通常の社会生活で個人を同定するための情報であり、通常は各個人の氏名が用いられるが、その他のもの（芸名，屋号，雅号など）であってもよい。

【００１１】本発明は以下の特徴をもつ。

【００１２】（イ）不特定多数の個人情報を集めて記憶する個人情報記憶手段と、記憶された特定の個人又は集団の個人情報にアクセスするために個人又は集団の個人識別符号を入力する識別符号入力手段と、個人情報にアクセスすることが正当であることを主張するアクセス権を入力するアクセス権入力手段と、各入力手段から入力されたアクセス権と個人識別符号を照合し、アクセスが正当か否かを判定するアクセス権判定手段と、アクセス権判定手段の判定結果に基づき個人情報記憶手段へのア

5

クセス又は情報記憶手段からの出力を制限するアクセス制限手段とを備え個人情報への不当なアクセスを防止する個人情報保護方法において、個人情報記憶手段は各個人を社会的に識別する公的個人識別情報と各個人に固有の私的情報とを含み、アクセス制限手段は公的個人識別情報と私的情報について各々独立にアクセス制限を行なう公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とからなり、アクセス権判定手段は、各入力手段から入力されたアクセス権と個人識別符号を照合した結果、公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与える個人情報保護方法に特徴を有する。

【００１３】（ロ）アクセス権入力手段は、患者が携帯し個人識別符号を保持する患者識別媒体から個人識別符号を入力する第１のアクセス権入力手段および医師が携帯しアクセス権を保持する医師識別媒体からアクセス権を入力する第２のアクセス権入力手段の二つからなり、アクセス権判定手段は、第１のアクセス権入力手段から入力された第１の個人識別符号と、識別符号入力手段から入力された第２の個人識別符号と、第２のアクセス権入力手段から入力されたアクセス権との合計３者からなる組合せに従って公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与えることを特徴とする。

【００１４】（ハ）アクセス権判定手段は、第１の個人識別符号と第２の個人識別符号とが入力され、かつ両者が異なる場合は公的個人識別情報と私的情報との双方へのアクセスを制限すること、第１の個人識別符号と第２の個人識別符号とが双方入力され、かつ両者が一致する場合はアクセス権の入力状況に従って、アクセス権が入力されない場合は、私的情報へのアクセスを制限し、アクセス権が入力された場合は、公的個人識別情報と私的情報双方に対しアクセスを制限しないこと、および第１の個人識別符号が入力されない場合はアクセス権の入力状況に従って、アクセス権が患者の主治医のアクセスであることを主張する場合には、公的個人識別情報と私的情報双方に対しアクセスを制限せず、アクセス権が主治医以外の者のアクセスであることを主張する場合には、公的個人識別情報へのアクセスを制限し、公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与えることを特徴とする。

【００１５】（ニ）各個人を社会的に識別する公的個人識別情報と各個人に固有の私的情報とを含む個人情報記憶装置と、特定の個人又は集団の個人情報にアクセスするために個人又は集団の個人識別符号を入力する識別符号入力装置と、個人情報にアクセスすることが正当であることを主張するアクセス権を入力するアクセス権入力装置と、公的個人識別情報へのアクセスを制限する公的個人識別情報アクセス制限装置と、私的情報へのアクセスを制限する私的情報アクセス制限装置と、各入力装置

6

から入力されたアクセス権と個人識別符号を照合した結果、公的個人識別情報アクセス制限装置と私的情報アクセス制限装置とに独立のアクセス権判定結果を与えるアクセス権判定装置とを備えた個人情報保護装置に特徴がある。

【００１６】（ホ）患者が携帯し個人識別符号を保持する患者識別媒体から個人識別符号を入力する第１のアクセス権入力装置と、医師が携帯しアクセス権を保持する医師識別媒体からアクセス権を入力する第２のアクセス権入力装置と、第１のアクセス権入力装置と、医師が携帯しアクセス権を保持する医師識別媒体からアクセス権を入力する第２のアクセス権入力装置と、第１のアクセス権入力装置から入力された第１の個人識別符号と、識別符号入力装置から入力された第２の個人識別符号と、第２のアクセス権入力装置から入力されたアクセス権とからなる組合せに従って公的個人識別情報アクセス権制限装置と私的情報アクセス権制限装置とに独立のアクセス権判定結果を与えるアクセス権判定装置とを備えた個人情報保護装置に特徴がある。

【００１７】

【作用】上記構成によれば、公的個人識別情報と私的情報とに対し、独立にアクセスの制限が行なえる。従って、公的個人識別情報（氏名）を秘匿したまま私的情報（医療データ）を利用できるので、患者のプライバシーを保ちながら医学研究を行なうことが可能である。またアクセス権入力手段が、患者が携帯し個人識別符号を保持する患者識別媒体から個人識別符号を入力する第１のアクセス権入力手段と、医師が携帯しアクセス権を保持する医師識別媒体からアクセス権を入力する第２のアクセス権入力手段の２者からなる場合は、第１のアクセス権入力手段から入力された第１の個人識別符号と、識別符号入力手段から入力された第２の個人識別符号と、第２のアクセス権入力手段から入力されたアクセス権との合計３者からなる組合せに従ってアクセス制限を決定することにより、氏名入りの医療データが漏洩することを患者自身が防止することが可能になる。

【００１８】

【実施例】図１は本発明の第１の実施例を示す。医師が患者の医療データにアクセスする場合は、まず識別符号入力手段２０から患者の識別符号を入力する。ここで識別符号としては通常、病院が患者管理のために設定する患者ＩＤ番号が用いられる。識別符号は記憶手段１０に送られ、公的個人識別情報１１および私的情報１２がアクセスされる。識別符号は同時にアクセス権判定手段４０にも送られる。

【００１９】次に医師はアクセス権入力手段３０を用いて、自分が患者の医療データにアクセスすることが正当であることを示すアクセス権情報を入力する。アクセス権情報は医師自身の氏名，暗証番号などが用いられる。アクセス権情報はアクセス権判定手段４０に送られる。

【００２０】入力手段２０，３０には汎用計算機用のキーボードを利用できるが、他の手段（カードリーダなど）でも良い。またこれら二つの入力手段には物理的には同一の装置を用いても良い。

【００２１】アクセス権判定手段４０はこれらの入力情報からアクセスの正当性を判定し、公的個人識別情報アクセス判定結果４１および私的情報アクセス判定結果４２を出力する。この判定は、例えば、下記（１）～（３）の規則で行なう。

【００２２】（１）アクセス権情報が患者の主治医であることを示す場合には、公的個人識別情報１１および私的情報１２双方へのアクセスが正当であると判定し、４１，４２双方に「アクセス可」を出力する。

【００２３】（２）アクセス権情報が患者の主治医を除く一般の医師である場合には、私的情報１２（医療データ）へのアクセスのみが正当であると判定し、４１には「アクセス不可」を、４２には「アクセス可」を出力する。

【００２４】（３）上記（１），（２）いずれでもない場合には、すべてのアクセスを正当ではないと判定し、４１，４２双方に「アクセス不可」を出力する。

【００２５】以上により作られた二つのアクセス判定結果４１，４２は、公的個人識別情報アクセス制限手段５１および私的情報アクセス制限手段５２に入力され、両制限手段は同入力に応じて公的個人識別情報および私的情報各々の出力を停止することでアクセスの制限を行なう。なお二つの制限手段５１，５２は、図４に示す様に公的個人識別情報および私的情報各々への個人識別符号入力を禁止する形式であってもよい。

【００２６】５１，５２を経た公的個人識別情報および私的情報は、合成手段１００により適当な書式に合成された後表示手段１０１に出力される。出力としてはＣＲＴ画面への表示，印刷，他の計算機システムへの伝送等が通常行なわれるが、他の方法でも良い。

【００２７】図２は本発明の第２の実施例を示したものである。本実施例が第１の実施例と異なる点は以下の二つである。

【００２８】（１）アクセス権入力手段３０が二つの入力手段３１および３２に分かれている。第１のアクセス権入力手段３１からは、患者が携帯し個人識別符号を保持する患者識別媒体から個人識別符号を入力し、第２のアクセス権入力手段３２からは、医師が携帯しアクセス権を保持する医師識別媒体からアクセス権を入力する。

【００２９】（２）アクセス権判定手段は、第１のアクセス権入力手段から入力された第１の個人識別符号と、識別符号入力手段から入力された第２の個人識別符号と、第２のアクセス権入力手段から入力されたアクセス権との合計３者からなる組合せに従って公的個人識別情報アクセス制限手段と私的情報アクセス制限手段とに独立のアクセス権判定結果を与える。ここで、アクセス権の判定は、たとえば下記（１）～（３）に記す規則により行なう。

【００３０】（１）第１の個人識別符号と第２の個人識別符号とが双方入力され、かつ両者が異なる場合は、公的個人識別情報と私的情報との双方へのアクセスを制限する。

【００３１】（２）第１の個人識別符号と第２の個人識別符号とが双方入力され、かつ両者が一致する場合は、アクセス権の入力状況に従って下記の規則でアクセスを制限する。

【００３２】（２－１）アクセス権が入力されない場合は、私的情報へのアクセスを制限する。

【００３３】（２－２）アクセス権が入力された場合は、公的個人識別情報と私的情報双方に対しアクセスを制限しない。

【００３４】（３）第１の個人識別符号が入力されない場合は、アクセス権の入力状況に従って次の規則でアクセスを制限する。

【００３５】（３－１）アクセス権が患者の主治医のアクセスであることを主張する場合には、公的個人識別情報と私的情報双方に対しアクセスを制限しない。

【００３６】（３－２）アクセス権が主治医以外の者のアクセスであることを主張する場合には、公的個人識別情報へのアクセスを制限する。

【００３７】本実施例によれば、患者が第１のアクセス権入力手段３１からのアクセス権情報入力を拒否することにより、自身の医療データが氏名入りで漏洩することを防ぐことが出来る。また、医師が不在であっても、患者は自己の医療データが記憶装置に記憶されているか否かを確認できる。なお、第１のアクセス権入力手段３１からのアクセス権情報入力は、患者が病院の診察券をカード読み取り装置から読ませる様にするのが運用上便利である。同様に第２のアクセス権入力手段３２からのアクセス権情報入力は、医師が自分の身分証明カードをカード読み取り装置から読ませる様にするのが運用上便利である。

【００３８】さらに最近は、患者の医療データを高密度記録媒体（磁気ディスクなど）に生涯にわたって蓄積し、患者に携帯させていろいろな医療機関で共通利用するシステムの実用化が試みられている。この記録媒体（健康手帳を電子化したものとみなせる）はその性格上患者のＩＤカードの機能をもつので、同媒体を第１のアクセス権入力手段３１に装着することによりアクセス権情報入力がなされたとみなすことができる。

【００３９】以上で述べた個人情報保護方法を応用することで、患者のプライバシー保護機能が必須である電子カルテシステムを実現することができる。

【００４０】

【発明の効果】本発明によれば、患者のプライバシー保護と医学研究との双方に有効な個人情報保護方法および

9

その装置が構成できる。

【図面の簡単な説明】

【図１】本発明の第１の実施例を示すブロック図。

【図２】本発明の第２の実施例を示すブロック図。

【図３】従来の個人情報保護方法を示すブロック図。

【図４】本発明のアクセス制限手段の他の実施例を示す＊

10

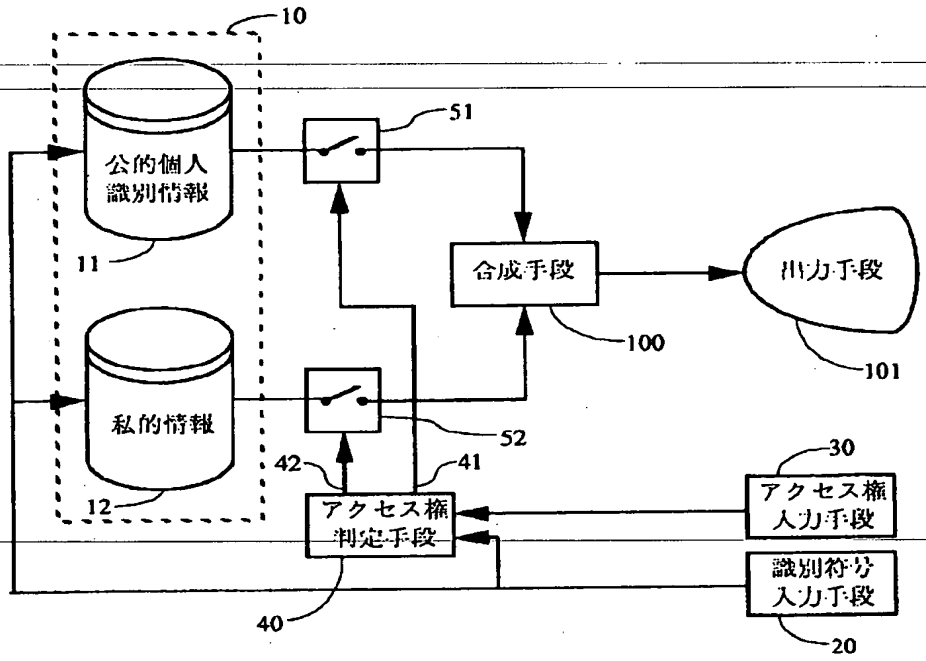
＊ブロック図。

【符号の説明】

１０…記憶手段、１１…公的個人識別情報、１２…私的情報、２０…識別符号入力手段、３１，３２…アクセス権入力手段、４０…アクセス権判定手段、４１，４２…判定結果、５１，５２…アクセス制限手段。

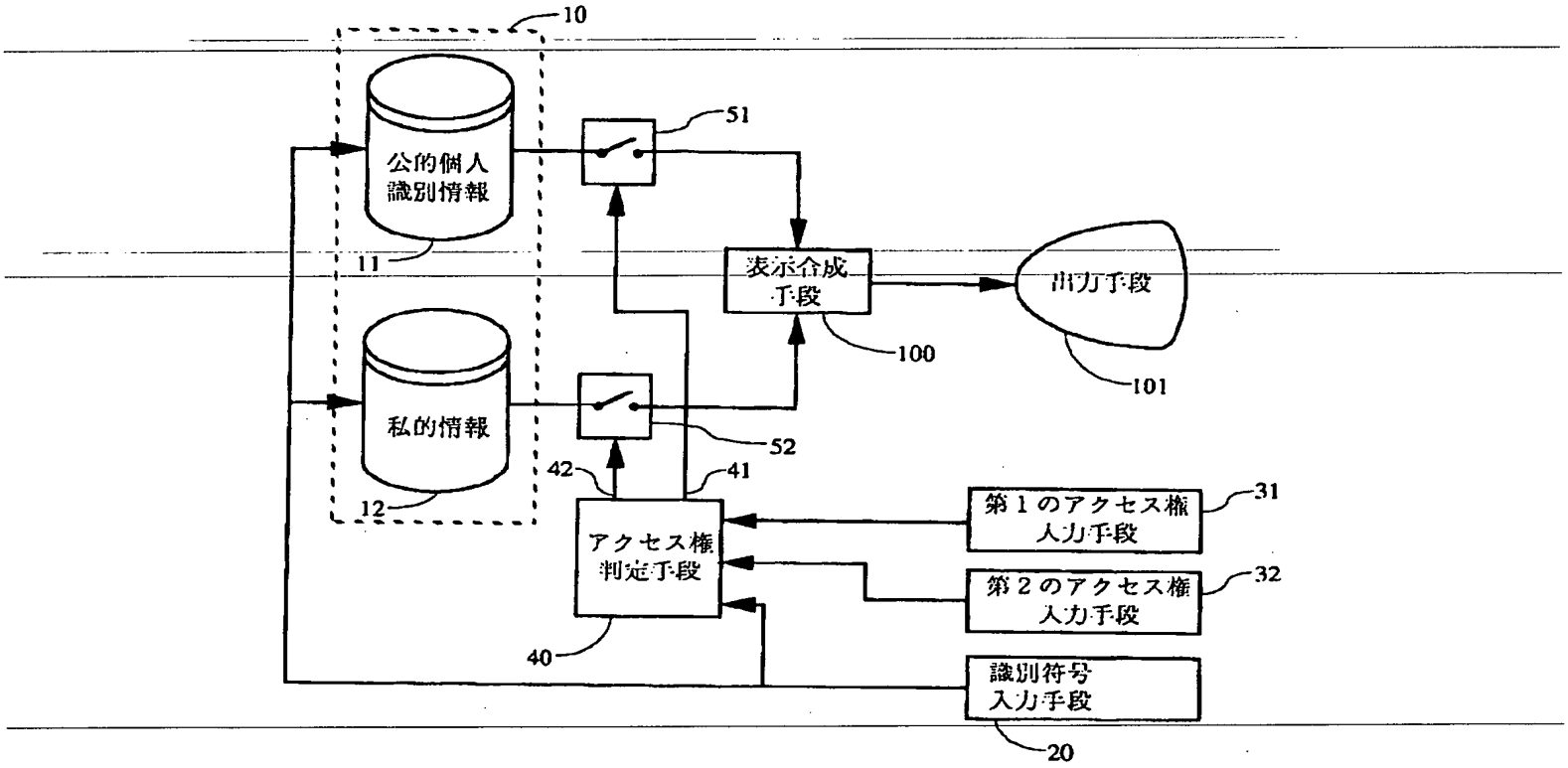
【図１】

図１



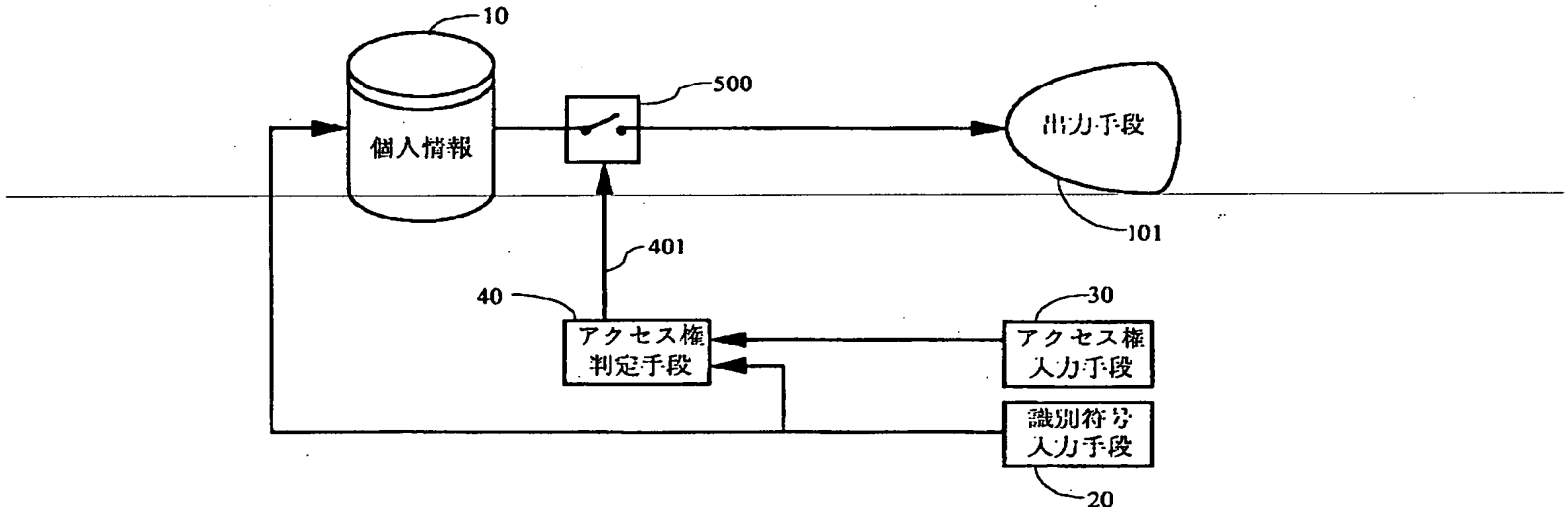
【図2】

図2



【図3】

図3



【図4】

図4